Exhibit 6

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	Docket No. 20-cr-10012-IT
	)	
v.	)	***LEAVE TO FILE REDACTED MEMO & EXHIBITS A-G, I-J UNDER SEAL GRANTED ON 12/27/21***
	)	
	)	
PAUL BATEMAN	)	

MOTION TO SUPPRESS EVIDENCE

The defendant, Paul Bateman, pursuant to Fed. R. Crim. P. 12 and the Fourth Amendment, respectfully moves this Court to suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant issued in this case because the warrant was not supported by probable cause. Mr. Bateman also moves for a *Franks* hearing, as the affiant made material misstatements that were necessary to a finding of probable cause and omissions that, if included in the affidavit, would have vitiated probable cause.

STATEMENT OF FACTS[1]

I. The Search Warrant

On December 11, 2019, Homeland Security Investigations ("HSI") Special Agent Gregory Squire submitted an application for a search warrant to the U.S. District Court of Massachusetts. *See* Search Warrant Affidavit (attached as Exhibit A). Agent Squire sought authorization to search Mr. Bateman's home located in Bridgewater, Massachusetts for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Attempted Receipt of Child Pornography) and 2252A(a)(5)(B) and (b)(2) (Access with Intent to View and Possession of Child Pornography, and attempt). Ex. A at ¶ 4.

[1] The facts in this section are drawn from the discovery provided by the government. By repeating the facts here, Mr. Bateman does not adopt them as true.

The affidavit submitted in support of the search warrant contains just one allegation of criminal activity. Specifically, Agent Squire stated:

> In the course of this investigation, a foreign law enforcement agency (hereinafter, "FLA") known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that FLA had determined that on April 30, 2019 at 10:38:18 UTC, IP address 73.142.30.140 was used to access online child sexual abuse and exploitation material via a website.

Id. at ¶ 23. Agent Squire went on to state that "[a]ccording to the FLA, the website had an explicit focus on the facilitation of sharing child abuse materials (images, links and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children." *Id*. He noted that "[u]sers were required to create an account (username and password) in order to access the majority of the material." *Id*. Furthermore, he stated that the "FLA provided further documentation naming the site…as Website A".[2] *Id*. The affidavit did not include any allegations that the IP address was used to create an account on the website in question. Nor did it include any information about what material was allegedly "accessed" or what section of the website the internet user associated with that IP address had visited.

Agent Squire claimed that Website A was a "child pornography online bulletin board dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children" that operated from around September 2016 to June 2019. *Id*. at ¶ 14-15. Noticeably absent from the affidavit, but ultimately disclosed by the government and otherwise known from cases arising out of the same investigation, is that Website A's operation ceased in June 2019, when its server was seized by an as-yet-unidentified FLA.[3]

---

[2] Agent Squire noted in the affidavit that the FLA "referred to the site by its actual name, not the pseudonym [Website A] used for the purposes of this warrant." Ex. A at ¶ 23, fn. 7. The government has since disclosed that the website was called [redacted]

[3] *See e.g. United States v. Kiejzo*, 4:20-cr-40036-TSH, D.E. 117-1 at pg. 3 (D. Mass. Oct. 19, 2021). The government in the instant case confirmed that both the instant case and *Kiejzo* arose out of the same

Agent Squire explained that Website A was a "hidden service" website that operated on the Tor network, a free and legal computer network "available to internet users that is designed specifically to facilitate anonymous communication over the internet." *Id*. at ¶ 6, 11. Agent Squire also included a description of how the Tor network operates and how information is anonymized on the network. *Id*. at ¶ 7-13. Specifically, Agent Squire noted that "the Tor network attempts to [facilitate anonymous communication over the internet] by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a 'circuit.'" *Id*. at ¶ 6. Agent Squire acknowledged that because of this process, "traditional IP address-based identification techniques are not effective." *Id*.

In the section of the affidavit discussing the tip, Agent Squire claimed that the FLA advised "that it had obtained that information through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws." *Id*. at ¶ 25. In a footnote, Agent Squire averred that the FLA (since identified as the [redacted]) was a "national law enforcement agency of a country with an established rule of law" and that there was a "long history of U.S. law enforcement sharing criminal information with FLA and FLA sharing criminal investigation information with U.S. law enforcement." *Id*. at ¶ 23, fn. 6. He further noted that the FLA had "advised U.S. law enforcement that FLA had not interfered with, accessed, search or seized any data from any computer in the United States in order to obtain that IP address information." *Id*. at ¶ 25. He averred that "U.S. law enforcement did not participate in the investigative work through which FLA identified the IP address." *Id*. Finally, Agent Squire alleged that prior tips provided by the FLA had "(1) led to the identification and arrest of a U.S.-

investigation, and also confirmed via email in December 2021 after specific inquiry that there was another, separate FLA local to the server host country that conducted the seizure of Website A's server – an FLA distinct from the tip-providing FLA referenced throughout Agent Squire's affidavit.

based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession." *Id*. at ¶ 26. Again, these averments were only made with respect to the tip-providing FLA, as there was no such mention or averment made as to the as-yet-unidentified FLA that seized the server.

According to the affidavit, the only thing that U.S. law enforcement did in response to the tip from the FLA was to send a subpoena to Comcast Communications for subscriber information related to the IP address. *Id*. at ¶ 27. Comcast provided law enforcement with a physical address – [redacted] – associated with the IP address. *Id*. Agent Squire, after reviewing commercial databases, property records, and RMV records, indicated that Mr. Bateman owned a condo at that address and that he resided there with an adult female. *Id*. at ¶ 28-29. Agent Squire also noted that on December 10, 2019, an HSI Task Force officer conducted surveillance on the condo and observed the cars at the residence that were registered to Mr. Bateman and the woman who allegedly lived with him. *Id*. at 29-30.

A search warrant to search Mr. Bateman's home was issued on December 11, 2019. *See* Search Warrant (attached as Exhibit C). The warrant was executed the next day. Based on the evidence discovered at Mr. Bateman's home, Mr. Bateman was arrested and a complaint was filed alleging violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) (receipt and possession of child pornography). On January 16, 2020, Mr. Bateman was charged via indictment with one count of receipt of child pornography and one count of possession of child pornography.

II. Information Recently Disclosed by the Government

On December 20, 2021, in response to a specific request by the defense, the government disclosed to defense counsel that the FLA that provided the tip to U.S. law enforcement (now known to be the [redacted]) and the FLA that seized the server that hosted Website A were not just different FLAs, but from different countries altogether. The government further disclosed that the FLA that seized the server was local to the server host country (not [redacted]). The government has declined to identify the second FLA or the server host country. None of this information was included in Agent Squire's affidavit.

ARGUMENT

I. The Warrant Was Not Supported By Probable Cause.

The Fourth Amendment of the United States Constitution guarantees the right to be secure against "unreasonable searches and seizures" and requires that no warrants issue "but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched." U.S. Const. Am. IV. "With limited exceptions, it requires police officers to secure a search warrant supported by probable cause prior to effecting a search or seizure." *United States v. Gifford*, 727 F.3d 92, 98 (1st Cir. 2013).

Probable cause to issue a search warrant exists when "given all the circumstances set forth in the affidavit … there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Id*. at 239. This Court is tasked with "ensur[ing] that the magistrate had a substantial basis for ... concluding that probable cause existed." *Id*. at 238-39.

When an affidavit relies on information provided by a confidential informant, "the affidavit must provide some information from which a magistrate can credit the informant's credibility." *Gifford*, 727 F.3d at 99. The First Circuit applies the following non-exhaustive factors in assessing probable cause:

> (1) whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information; (2) whether an informant's statements reflect first-hand knowledge; (3) whether some or all of the informant's factual statements were corroborated wherever reasonable or practicable (e.g., through police surveillance); and (4) whether a law enforcement affiant assessed, from his professional standpoint, experience, and expertise, the probable significance of the informant's provided information.

United States v. Tiem Trinh, 665 F.3d 1, 10 (1st Cir. 2011).

Here, the affidavit submitted in support of the search warrant failed to establish a "fair probability" that evidence of a crime would be found in Mr. Bateman's home. *Gates*, 462 U.S. at 238-39. The affidavit relied entirely on one unsubstantiated and stale allegation of criminal activity by an unidentified foreign law enforcement agency. The affidavit failed to include any information as to how the FLA came across that information, how reliable the method the FLA used to obtain the information was, and whether the IP address was obtained through first-hand knowledge or through other sources. Without more information about the source of the FLA's tip and without additional corroboration, the months-old tip was not sufficient to establish probable cause, and Agent Squire could not possibly have assessed the probable significance of the tip.

a. The Tip Was Insufficient To Establish Probable Cause.

The factors outlined by the First Circuit in *Tiem Trinh*, 665 F.3d at 10, are instructive in this case because the tip that forms the entire basis of probable cause in the affidavit came from a confidential source akin to an informant. Those factors, although non-exhaustive, weigh in Mr. Bateman's favor. Agent Squire's affidavit is deficient because 1) it fails to establish the basis of

knowledge for the tip and whether it was obtained through first-hand knowledge or through hearsay (factors 1 and 2 in the *Tiem Trinh* analysis), and 2) it reflects no attempts from any U.S. law enforcement agency to corroborate the tip from the unidentified FLA (factor 3 of *Tiem Trinh*).

i. The Affidavit Fails to Establish the Basis of Knowledge for the Tip.

The affidavit is deficient because it failed to establish the basis of knowledge for the tip in two respects. First, Agent Squire did not include any information about whether the tip was obtained through first-hand knowledge or through hearsay. Second, Agent Squire included no facts about the method used to obtain the IP address information and whether that method was reliable.

The only information provided in the affidavit that offered any clues about the source of the FLA's tip were Agent Squire's statements that the FLA "had obtained [the information in the tip] through independent investigation that was lawfully authorized in FLA's country pursuant to its national laws," and that "FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." Ex. A, ¶ 25. However, neither statement by Agent Squire was sufficient to assure the Magistrate of the tip's reliability. Agent Squire did not state that the IP address information had reached the FLA through a reliable first-hand source rather than through multiple layers of hearsay. *Cf. Gates*, 462 U.S. at 234 (noting that the informant's "explicit and detailed description of alleged wrongdoing, along with a statement that the event was observed *first-hand*, entitles his tip to greater weight than might otherwise be the case"); *United States v. Taylor*, 985 F.2d 3, 5-6 (1st Cir. 1993) (noting that an affidavit may support an informant's veracity "through the very specificity and detail with which it relates the informant's *first-hand* description of the place to be searched or the items to be seized"). Nor did Agent Squire aver that *no* FLA had "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. A, ¶ 25. Instead, Agent Squire left the

Magistrate to guess at how the FLA had obtained the information and to merely ratify Agent Squire's conclusion that the tip was a reliable one.

The First Circuit has found that a lack of explanation of the basis of knowledge for an informant's tip undermines a finding of probable cause. *Gifford*, 727 F.3d at 99-101. In *Gifford*, an informant told the affiant that the defendant was growing marijuana at his house. *Id*. at 95. However, the affidavit included no information about the informant's basis of knowledge for the tip. It was therefore unclear "whether the informant just happened to view the grow operation, heard about it as hearsay, or had direct, first-hand knowledge of the grow operation in the Gifford home." *Id*. at 100. Because the affidavit lacked any "statements as to the informant basis of knowledge," there was no means for the magistrate to determine "whether that information was obtained first-hand or through rumor." *Id*. The lack of any information about the source of the informant's knowledge weighed against a reliability finding in *Gifford*.

The facts of this case mirror those in *Gifford* and compel the same conclusion. As in *Gifford*, it is entirely unclear how, when, and through what method the FLA that provided the tip learned about the IP address. Without that information, there was no basis for the magistrate to determine whether the content of the tip from the FLA was reliable and trustworthy. By not divulging any information about the FLA's basis of knowledge, the magistrate was left with no reason to believe that the tip was obtained through a reliable and trustworthy source or method. Simply repeating the FLA's allegation without further explaining how the FLA uncovered the connection between the IP address and the accessing of child sexual abuse material was insufficient to adequately establish the basis of knowledge of the tip. The first and second factors of *Tiem Trinh* – "whether the affidavit establishes the probable veracity and basis of knowledge of persons

supplying hearsay information" and "whether an informant's statements reflect first-hand knowledge" – therefore weigh in Mr. Bateman's favor. *Tiem Trinh*, 665 F.3d at 10.

ii. The Affidavit Reflects No Effort From Law Enforcement To Corroborate The Tip.

In addition to the lack of information about the basis of knowledge or reliability of the method used to obtain the IP address, the affidavit does not include any facts that actually or meaningfully corroborated the tip from the FLA that an internet user had "accessed online child sexual abuse and exploitation material via a website." Ex. A, ¶ 23. While Agent Squire did include a description of the steps U.S. law enforcement took to confirm who lived at [redacted], that investigation only corroborated the fact that someone lived at the physical address associated with the IP address identified by the FLA. None of that investigation corroborated the tip that that particular IP address was used to access child pornography on April 30, 2019.

In the affidavit, Agent Squire briefly detailed the steps agents took to identify who, if anyone, lived at [redacted]. They deduced, according to the affidavit, that Mr. Bateman owned a condominium at that address, that he listed [redacted] as his residential and mailing address at the RMV, and that he resided there with an adult woman. Ex. A, ¶ 27-30. One agent also saw cars that were registered to Mr. Bateman and the woman who resided there with him parked in front of the condo one day before the warrant was submitted to the Magistrate. *Id*. While this information certainly may have substantiated a claim that Mr. Bateman lived at that address in December 2019, none of it corroborated the allegation made by the FLA – that an internet user at [redacted] had accessed child sexual abuse material in April 2019. *See Gifford*, 727 F.3d at 99-102 (DMV records that confirmed the defendant lived at his address did not corroborate an informant's tip that there was an ongoing grow operation at that address). The third factor identified in *Tiem Trinh* – "whether some or all of the informant's factual statements were

corroborated wherever reasonable or practicable" – therefore weighs in favor of Mr. Bateman. *Tiem Trinh*, 665 F.3d at 10.

In sum, Agent Squire failed to establish the basis of knowledge for the tip or the reliability of the method used to obtain the information in the tip. Agent Squire also failed to include any facts that corroborated the unreliable tip. The information provided in the affidavit therefore did not create a "substantial basis" for the magistrate to conclude that probable cause existed. *Gates*, 462 U.S. at 238-39.

b. The Warrant Was Stale.

Stale information cannot establish probable cause that evidence of criminal activity will be found at the place searched. *United States v. Grubbs*, 547 U.S. 90, 96 n.2 (2006). Whether information is stale does not depend solely on the number of days between the events described in the affidavit and the issuance of the warrant. *Tiem Trinh*, 665 F.3d at 13–14. Courts look instead at a number of factors, including "the nature of the information, the nature and characteristics of the suspected criminal activity, and the likely endurance of the information." *Id.* (citing *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008)). In cases involving child pornography, courts have often determined that the passage of a significant amount of time between the acquisition of the incriminating information and the obtaining of a warrant does not render the information stale where the magistrate was provided with information supporting a finding that such materials are likely to have been retained by their possessor. *See, e.g., Morales-Aldahondo*, 524 F.3d at 119.

Here, the FBI did not have probable cause to search Mr. Bateman's home in December 2019 when the alleged access to child sexual abuse material occurred in April 2019 – seven months earlier. The affidavit did not include any allegations specific to Mr. Bateman regarding any

propensity or habits of keeping a collection of child pornography. Moreover, the affidavit failed to state what exactly was accessed on the website, whether it was downloaded or saved in any manner, or whether there were multiple visits to the website – facts that could have bolstered probable cause. *See United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015) (no probable cause where the affidavit alleged that "on a single afternoon more than nine months earlier, a user with an IP address associated with Raymonda's home opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files").

Without more information specific to Mr. Bateman, and without more information about the material allegedly viewed and the number of visits to the website, there was not probable cause to believe that Mr. Bateman's home contained evidence of a crime. The warrant was unlawfully issued, and all evidence obtained as a result of the search conducted pursuant to the warrant must be suppressed.

II. The Affiant Made Material Omissions and Misstatements and Mr. Bateman is Entitled to a *Franks* Hearing as a Result.

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or [made] with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). "An allegation is made with reckless disregard for the truth if the affiant in fact entertained serious doubts as to the truth of the allegations or where circumstances evinced obvious reasons to doubt the veracity of the allegations in the application." *Gifford*, 727 F.3d at 98 (internal quotations omitted). "Suppression of the evidence seized is justified if, at such a hearing, the defendant proves intentional or reckless

falsehood by preponderant evidence and the affidavit's creditworthy averments are insufficient to establish probable cause." *United States v. Tanguay*, 787 F.3d 44, 49 (1st Cir. 2015).

The right to a Franks hearing is triggered not only by false statements but also by material omissions. *Id.*; *United States v. Cartagena*, 593 F.3d 104, 112 (1st Cir. 2010). When a defendant alleges a material omission has been made, "[t]he required showing is two-fold: first, the omission must have been either intentional or reckless; and second, the omitted information, if incorporated into the affidavit, must be sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. The First Circuit has held that recklessness may be inferred where "the omitted information was critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100.

Special Agent Squire made omissions and misstatements knowingly and intentionally, or with reckless disregard for the truth regarding three key issues. First, Agent Squire made material misstatements about the nature, origin, and reliability of the tip from the FLA. Second, Agent Squire made material omissions about the method(s) used by the FLA to identify the IP address. Third, Agent Squire misrepresented the relationship between U.S. law enforcement and the FLA in the affidavit. Each of these misstatements and misrepresentations went directly to the heart of the probable cause analysis. The magistrate would not have issued the warrant had these misrepresentations been corrected in the affidavit because the reformed affidavit would not establish probable cause. Mr. Bateman is therefore entitled to a *Franks* hearing.

a. Agent Squire Misrepresented the Nature, Origin, and Reliability of the Tip.

The affidavit relies entirely on Agent Squire's assertion that an FLA notified U.S. law enforcement that a particular IP address "was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website A." Ex. A, ¶ 23. There is no other allegation of criminal activity anywhere in the affidavit. However, this fact is

inherently misleading and factually incorrect. Agent Squire did not repeat the tip from the [redacted] verbatim. Rather, he added language that misled the magistrate into believing that U.S. law enforcement had more evidence of criminal activity that it did.

The exact words of the tip from the [redacted] tip document were: "[redacted]" *See* [redacted] Intelligence Report (attached as Exhibit D). Agent Squire did not copy or repeat this language into the affidavit. Instead, he stated the following: "FLA had determined that on April 30, 2019 at 10:38:18 UTC, IP address 73.142.30.140 was used to access online child sexual abuse and exploitation material *via a website*. According to the FLA, the website had an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on BDSM, hurtcore, gore, and death-related material including that of children. Users were required to create an account (username and password) in order to access the majority of the material." Ex. A, ¶ 23.

While this change appears slight, its significance in the affidavit was great. By manipulating the language of the tip, Agent Squire created the impression that the [redacted], and therefore U.S. law enforcement, had information that the IP address was used to visit Website A *and then used to access child sexual abuse material*. The implication in the affidavit is that the internet user associated with that IP address viewed or downloaded the child sexual abuse material available on Website A and that, because the majority of the material was only available through an account, the internet user had accessed the child sexual abuse material through that account.

However, this implication misrepresents the substance of the tip from the [redacted] The [redacted] did not provide any such information, nor did U.S. law enforcement have any such evidence. Rather, the tip from the [redacted] conveyed only that the IP address in question was used to *access the website*.

The phrasing of the [redacted] Intelligence Report supports this interpretation of the tip. In the Intelligence Report, the [redacted] states that the IP address was used to "access online child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material." Ex. D. The tip is inscrutable as it is written because it is unclear how "child sexual abuse and exploitation material" (i.e., videos and images) can have an "explicit focus" on the *facilitation of sharing the same material*. Its meaning only becomes clear if the phrase "online child sexual abuse and exploitation material" means Website A, rather than images or videos depicting child sexual abuse. In other words, the Intelligence Report should be read as "On 2019-04-30 10:38:18 UTC 73.142.30.140 was used to access [Website A], with an explicit focus on the facilitation of sharing child abuse material (images, links, and videos), emphasis on BDSM, hurtcore, gore and death-related material including that of children." This reading is consistent with, and tracks the exact language of, the [redacted] Intelligence Report identifying the website, which uses the identical language to describe the *website itself*, not the activity of the internet user. *See* Ex. F.[4]

Other parts of the affidavit reflect that this was, and has been, U.S. law enforcement's understanding of the [redacted] tip. *See* Ex. A at ¶ 24 ("I submit that the **website accessed by the IP address** 73.142.30.140 appears to be Website A."); ¶ 27 ("According to publicly available information, IP address 73.142.30.140 – the one used to **access Website A**… is owned/operated by Comcast."); ¶ 39 ("I am aware that this investigation revealed that an individual located at the

[4] The images and videos named in Ex. F appear to be those shared on the website, *not those accessed, viewed, or downloaded by any one user, let alone Mr. Bateman.*

address listed in Attachment A **accessed a website** that is dedicated to the sexual exploitation of children, and which is accessed through the Tor network.").

In rewording the tip from the [redacted], Agent Squire also omitted the crucial fact that the homepage of Website A did not contain any child sexual abuse material. Screenshots of the website provided by the government show that in order to "access" any child sexual abuse material, an individual would have to navigate past the homepage and, as Agent Squire acknowledges, log in with a username and password to access the material in question. Contrary to the impression created by Agent Squire in the affidavit, the [redacted] did not state in its tip that it had any information that the internet user associated with that IP address had an account on Website A, nor did it state that the user had logged into the website using a username and password.

The distinction between the substance of the tip and the retelling of that tip in the affidavit is important. There is a fundamental difference between: 1) evidence of a one-time visit to a website where no images, videos, or links to child pornography materials were either visible or available on the website's homepage, and no such items were viewed and/or downloaded and 2) evidence of an individual creating an account on that website and then using that account to view, download, or possess materials that would have only been accessible once a user navigated past the homepage. *See United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008) (finding no probable cause for possession of child pornography when it was alleged that defendant "appear[ed]" to have "gained access or attempted to gain access" to the cpfreedom.com website—which did not require registering an account or logging in—and that even if one inferred that the defendant had accessed cpfreedom.com, there was no specific allegation that the defendant "accessed, viewed or downloaded child pornography"). The information the [redacted] relayed to U.S.

law enforcement fell squarely into the first category, which was insufficient to establish probable cause.

By manipulating the language in the tip from the [redacted], Agent Squire misrepresented the information available to U.S. law enforcement and created a misleading impression that U.S. law enforcement had more evidence of criminal activity than it actually did regarding the sole allegation of criminal activity in the affidavit. Agent Squire's misrepresentation about the nature of the tip was recklessly made and was "necessary to the finding of probable cause." *Franks*, 438 U.S. at 155-56. Had Agent Squire been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used on a single occasion to visit a website where no child pornography was visible or available on the homepage, the magistrate could not have found sufficient probable cause to issue the warrant. Mr. Bateman is therefore entitled to a *Franks* hearing on these false statements.

In addition to this misrepresentation about the nature of the tip from the [redacted], Agent Squire also omitted important information about the origin and reliability of the tip. In the affidavit, Agent Squire made a number of representations about the FLA that had provided the tip (now known to be the [redacted]) and its reliability. Specifically, Agent Squire stated that that FLA (again, [redacted]) had "a history of providing reliable, accurate information in the past" and that it was "a national law enforcement agency of a country with an established rule of law." Ex. A, ¶ 23. Agent Squire averred that the FLA (the [redacted]) had obtained the information in the tip through an investigation that was "lawfully authorized in FLA's country pursuant to its national laws," and that the FLA (the [redacted]) had not "interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain the IP address information." *Id*. at ¶ 25. Finally, Agent Squire

claimed that prior tips from the FLA (the [redacted]) had led to an arrest, the rescue of children subject to abuse, and the seizure of evidence. *Id*. at ¶ 26.

However, Agent Squire omitted from the affidavit the fact that there was not just one FLA involved in the investigation of Website A, but two, from two entirely different countries. The [redacted], which provided the tip to U.S. law enforcement and which Agent Squire took pains to assure the court was subject to the rule of law, was seemingly not involved in the seizure of the website's server. Instead, the government recently disclosed that a second FLA – which it has refused to name – seized the server in a country distinct from [redacted] – a country which it has also refused to name. Additional information – such as who participated in the seizure and/or investigation/investigation steps and what investigative steps were undertaken by the seizing FLA alone or in conjunction with other countries and/or law enforcement, including the United States – remains unknown. What little *is* known about the second FLA is that it was local to the server host country.

Agent Squire made no distinction between the two FLAs in the affidavit and failed to inform the court that there was even a second FLA involved in the investigation. Instead, Agent Squire created the misimpression that the tip and the source of that tip both originated from the same, allegedly reliable FLA. This impression was both misleading and inaccurate. While Agent Squire made a number of claims in the affidavit about the reliability of the FLA, those statements applied *only* to the FLA that provided the tip to U.S. law enforcement (again, [redacted]). There are no facts in the affidavit that address or establish the reliability or trustworthiness of the FLA that seized the server. Agent Squire did not, for example, make any assurances that the FLA that seized the server had a "history of providing reliable, accurate information." Nor did Agent Squire aver that the second FLA was from a country with an "established rule of law." Ex. A, ¶ 25. Likewise,

there are no facts in the affidavit that establish that the FLA that seized the server did not conduct a search or seizure of any computer in the United States (e.g. performing a so-called "Network Investigative Technique" (NIT)).

This misinformation went to the heart of the probable cause analysis. The tip from the [redacted] was the only allegation of criminal activity in the entire affidavit. It was also the only piece of information that created a nexus between Mr. Bateman, his home, and the alleged criminal activity. The omitted fact that there was a second FLA involved in obtaining the IP address information "require[s] that [this Court] alter in significant ways the weight [it] give[s] to" the tip. *Gifford*, 727 F.3d at 101. Without assurances in the affidavit about the reliability and trustworthiness of the second FLA and the legality of its action, no Magistrate could find there was probable cause.

Because Agent Squire's misrepresentations and omissions regarding the nature, origin, and reliability of the tip were all "critical to the probable cause determination," this Court "may infer recklessness" on the part of Agent Squire. *Gifford*, 727 F.3d at 101. The reckless misrepresentations were "necessary to the finding of probable cause" and the omitted information, adding back into the affidavit, "is sufficient to vitiate probable cause." *Franks*, 438 U.S. at 155-56; *Tanguay*, 787 F.3d at 49. Mr. Bateman is therefore entitled to a *Franks* hearing.

b. The Affiant Made Material Omissions Regarding The Method Used by the FLA to Identify the IP Address.

In the affidavit, Agent Squire stated that the FLA ([redacted]) assured U.S. law enforcement that that FLA had not "interfered with, accessed, searched, or seized any data from any computer in the United States." Ex. A, ¶ 25. This assurance, combined with the omitted fact that there was more than one FLA involved in the investigation, created the impression that no law enforcement agency, anywhere, had "interfered with, accessed, searched, or seized" data from a computer in the United States. However, an expert declaration submitted in a case seemingly identical to Mr.

Bateman's, and arising out of the same tip, suggests that the specific IP address could not have been identified without running a NIT or, in the alternative, an error-prone and unreliable traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2 (attached as Exhibit H).

In Professor Murdoch's declaration, he explains that "there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a Network Investigative Technique (which interferes with a user computer)." Ex. H, ¶ 23. A NIT works "by forcing the user's computer to disclose its IP address by connecting directly to a law-enforcement server without using the Tor network." *Id*. at ¶ 27. A NIT "necessarily interferes with a user's computer wherever it is located." *Id*. at ¶ 32.

Traffic analysis, on the other hand, is a technique that attempts to "identify which user is communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers)." *Id*. at ¶ 17. Professor Murdoch states that before 2016, "traffic analysis on Tor was unreliable, but there were concerns that it might be possible in some cases." However, in 2016, Tor addressed this issue and introduced a new extension to its software that caused traffic analysis to "introduce more errors, both false positives (where a user is incorrectly identified as having visited the Onion Service) and false-negatives (where a user is incorrectly identified as not having visited the Onion Service)." *Id*. at ¶ 19. This measure, and others, have made it "even more difficult to use traffic-analysis to de-anonymize Tor users." *Id*. at ¶ 21.

The use of either technique by [redacted] or another FLA would significantly undermine the veracity of the affidavit and its probable cause showing. If traffic analysis was used to uncover the IP address, the undisclosed fact that the technique is inherently error-prone would significantly

undermine the strength and reliability of the tip from [redacted]. *See id*. at ¶ 22-32. No magistrate, had he or she been aware that this fundamentally unreliable technique was used to obtain the IP address, would find there was probable cause, especially where the tip about the IP address was not corroborated by any other facts.

Alternatively, the use of a NIT would reveal a substantial misrepresentation in the affidavit, which relies on Agent Squire's assurance that no computer in the United States had been searched. The deployment of a NIT is an unlawful warrantless search. *See United States v. Tagg*, 886 F.3d 579, 584 (6th Cir. 2018); *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016), *aff'd*, 923 F.3d 1 (1st Cir. 2019). Had any law enforcement agency deployed a NIT to obtain the IP address without a warrant, the Magistrate could not have considered the results of that search in the probable cause analysis. *See United States v. Dessesaure*, 429 F.3d 359, 367 (1st Cir. 2005) ("[W]hen faced with a warrant containing information obtained pursuant to an illegal search, a reviewing court must excise the offending information and evaluate whether what remains is sufficient to establish probable cause.").

Agent Squire's omissions regarding the method used to obtain the IP address were material because if the omitted information – either that a NIT or an error-prone traffic analysis was used – was included in his affidavit, it would be "sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49. This Court may infer that the information was omitted recklessly because the omitted information was "critical to the probable cause determination." *Gifford*, 727 F.3d at 99-100. Mr. Bateman is therefore entitled to a *Franks* hearing on this issue as well.

c. The Affiant Misrepresented The Nature Of The Relationship Between U.S. Law Enforcement And The FLAs And Omitted Facts That Would Have Revealed that the FLAs' Actions Were Subject to the Exclusionary Rule.

Agent Squire's final misrepresentations involved omitting facts about the role of U.S. law enforcement in the investigation of Website A. Specifically, Agent Squire withheld information that would have shown that 1) U.S. law enforcement was engaged in a "joint venture" with the FLAs and 2) the FLAs engaged in conduct that would shock the judicial conscience such that the FLAs' actions would be subject to the exclusionary rule.

Generally, "the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures." *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). There are, however, two exceptions to that rule: "(1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*. Here, both exceptions would apply to the conduct of the FLAs. Running a NIT to obtain an IP address of a computer in the U.S. – conduct that is unlawful in the U.S. without first obtaining a warrant – and then hiding that information from a magistrate judge would "shock the judicial conscience." *Id*. Likewise, the information available to the defense suggests that there was a "joint venture" afoot between the United States and the FLAs such that the exclusionary rule would apply to one (or both) of the FLAs running a NIT on a computer in the United States. *See id*. However, Agent Squire minimized the collaborative relationship between the agencies and withheld facts that would have established that "American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." *Id*.

[redacted]

[redacted][5] [redacted]

[redacted]

[redacted]

[redacted][6] [redacted]

[redacted]

[redacted]

[redacted]

[redacted][7] [redacted]

[redacted]"[8] [redacted]

[redacted].[9]

Although the Affidavit indicates that "U.S. law enforcement personnel did not participate in the investigative *work* through which [redacted] identified the IP address information provided by

[5] *See* [redacted]

[6] *See* [redacted]

[7] *See* [redacted]

[8] *Id.*

[9] *See* [redacted]

[redacted],” Ex. A, ¶ 25, the [redacted]’s own representations about its collaborative work through its international liaison officers belie any conclusion that they solely engage in a simple information-sharing relationship with other countries. Specifically, [redacted][10]

Cases filed in this district and others demonstrate that the tips provided by [redacted] to U.S. law enforcement are more than just an informal, one-off relaying of information. *See, e.g., United States v. Kiejzo*, No. 1:20-cr-40036-TSH (D. Mass.); *United States v. Corwin*, No. 2:21-cr-00218-JS (E.D.N.Y.), D.E. 1 (unsealed at D.E. 4) (complaint affidavit indicates that in August 2019, the FBI received information from an FLA regarding an IP address which allegedly accessed [redacted] on April 27, 2019); *United States v. Sanders*, No. 1:20-cr-00143-TSE (E.D. Va.).

[redacted]”[11] [redacted]

[10] [redacted]

[11] *Id*.

[redacted][12] [redacted]

[redacted][13]

[redacted]"[14] [redacted]

[redacted]"[15]

The link between the U.S. and [redacted] in these kinds of operations is neither nebulous nor abstract – indeed, Agent Squire asserted that he was an "active member of a multinational, multi-agency working group that coordinates national and international operations to combat child exploitation on the dark web[.]" Ex. A, ¶ 1. The government, in a discovery response,

[12] *Id*.

[13] *Id*.

[14] See Twitter profile [redacted] and attached screenshots at Exhibit I.

[15] *See* "Justice News: Deputy Assistant Attorney General Richard W. Downing Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety," April 5, 2019 (emphasis added), available at: https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-academy-european-law (last accessed Dec. 10, 2021).

acknowledged that "there is at least one representative of the FLA in the working group." *See* Exhibit A to Defendant's Motion to Compel filed under seal at D.E. 76.

Based on the materials available to the defense, it appears there was, at the minimum, a significant collaboration between the United States and the [redacted]. By withholding this information from the affidavit, Agent Squire obscured the extent to which there was a "joint venture" between the two law enforcement agencies such that the actions taken by the [redacted] would be subject to the exclusionary rule. This information was material as the tip from the [redacted] formed the entire basis for probable cause in the affidavit. Mr. Bateman is therefore entitled to a *Franks* hearing on this misrepresentation.

Because the government has not disclosed the identity of the second FLA, the defense has been unable to investigate the possibility of a joint venture or cooperation between the United States and the second FLA. However, a recent case from the Northern District of Illinois, *United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020), sheds light on how U.S. law enforcement engages in these very kind of joint investigations of hidden services websites on Tor with FLAs and how that might have occurred in this case. In *Mitrovich*, the FBI began investigating a child pornography website in 2014. *Id*. at 963. Sometime that year, the FBI "obtained the ability to identify IP addresses associated" with the website, and learned that the website was hosted in the Netherlands, with the head administrator residing in Australia. *Id*. After the FBI shared that information with Australia, law enforcement agencies from Australia and New Zealand seized control of the website, operated it undercover, and shared backup copies of the website with the FBI. *Id*. As part of its investigation, the Australian and New Zealand authorities uploaded a hyperlink onto the website that, when clicked, allowed them to capture the clicker's IP address, which would have otherwise been concealed by Tor. *Id*. One particular user – known as

"cyberguy" – clicked on the hyperlink, thereby revealing his IP address, which was located in the United States, to the Australian and New Zealand authorities. *Id*. Australia and New Zealand sent the IP address to the FBI, which then obtained records from Comcast to identify the physical address associated with the IP address. *Id*. The FBI subsequently obtained a search warrant for that address – the defendant's home – and discovered child pornography materials therein. *Id*.

The facts in *Mitrovich* demonstrate how a U.S. law enforcement agency could *and did* participate in the seizure of a website server with an FLA. The facts also demonstrate that while U.S. agents may not necessarily direct an investigation into one particular IP address, a U.S. law enforcement agency could be engaged in a joint venture to uncover IP addresses within the United States. In *Mitrovich*, the court held that the defendant had made a *prima facie* showing that a Fourth Amendment search had taken place and that U.S. law enforcement was sufficiently involved to implicate the exclusionary rule such that the defendant was entitled to discovery on the issue. *Id*. at 967. Here, Mr. Bateman has made a substantial preliminary showing that Agent Squire omitted crucial information about the existence of a second FLA involved in the investigation of Website A. He has demonstrated that there was a joint venture between U.S. law enforcement and the [redacted], the only FLA so far identified by the government. The omissions and misrepresentations about the investigation into Website A by multiple FLAs and the relationship between those FLAs were material to probable cause and Mr. Bateman is entitled to a *Franks* hearing as a result.

CONCLUSION

For the above reasons, this Court should suppress all evidence and illegal fruits obtained pursuant to the invalid search warrant and grant Mr. Bateman a *Franks* hearing.

Respectfully submitted,
PAUL BATEMAN
By His Attorney,

/s/ Sandra Gant
Sandra Gant, BBO # 680122
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

/s/ Caitlin Jones
Caitlin Jones, MN ID # 0397519
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Sandra Gant, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on December 27, 2021.

/s/ Sandra Gant
Sandra Gant

UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Docket No. 20-cr-10012-IT
	)	
	)	
	)	
PAUL BATEMAN	)	

MOTION TO SUPPRESS

Exhibit H:

Declaration of Professor Steven Murdoch

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant	Case No.: 1:20-cr-00143

DECLARATION OF PROFESSOR STEVEN MURDOCH

I, Professor Steven Murdoch, Declare under penalty of perjury that:

1. I am currently Professor of Security Engineering at University College London. My research is focused on information security, particularly Internet privacy and payment systems security.
2. I have a Ph.D. from the Security Group of the University of Cambridge Department of Computer Science and Technology. My doctoral research, completed in 2007, focused on the traffic analysis of anonymous communications systems, in particular Tor. I have worked with the developers of Tor since 2004, and I created the first version of the Tor Browser software in 2008. I continue to work with the Tor Project, the 501(c)(3) non-profit organization responsible for the development of the Tor network and associated software. I helped the Tor Project assess and improve the security and usability of Tor.

3. I am a member of Christ's College Cambridge and a Royal Society University Research Fellow. I am a Fellow of the Institution of Engineering and Technology (IET) and the British Computer Society (BCS).
4. I have published a number of peer-reviewed research papers in the fields of anonymous communications and privacy-enhancing technologies, including Tor.
5. My CV is attached as Exhibit A.

Scope of declaration

6. This declaration will discuss how the Tor network operated and how activity on the Tor network could be traced as of May 23, 2019 – the date of the alleged visit in this case. I have restricted this declaration to the use of websites running as Tor Onion Services (also known as Tor Hidden Services), where the website is accessible only through the Tor network. I also will only discuss version 2 Tor Onion Services, in which the Onion Service address is 16 characters followed by ".onion" as the website in question for this case is a version 2 Onion Service (because according to a screenshot disclosed in discovery, its address had 16 characters before the ".onion," not 56).
7. The vast majority of usage of the Tor network (about 98% as of June 2021) is to visit websites and other Internet services which are also accessible directly over the Internet. I will not discuss this use of Tor in my declaration because it is not the type of usage alleged in this case. Similarly, I will not discuss version 3 Tor Onion Services, in which the Onion Service address is 56 characters followed by ".onion."

Operation of Tor Onion Services

8. When a user wishes to visit a Tor Onion Service, various computers (nodes) within the Tor network are involved. Some of these nodes are selected at random by the Tor software running on the user's computer, and the others are selected at random by the Tor software running on the Onion Service.
9. The Tor software on the user's computer will select at random a node to act as the rendezvous node and send the address of the rendezvous node to the Onion Service.

To protect the anonymity of the Onion Service (i.e., its IP address),[1] its connection is made through a three-node Tor circuit. Similarly, to protect the anonymity of the user, its connection to the rendezvous node is through a three-node Tor circuit.

10. Next, the Onion Service will connect to the rendezvous node through a three-node Tor circuit (excluding the rendezvous node). The rendezvous node is responsible for connecting together the two circuits: one created by the user's computer and one by the Onion Service. The Onion Service and user can then exchange information, i.e., the user's web browser can request to view a web page and other data, and the Onion Service can respond with the requested content, without disclosing each other's IP addresses.
11. When the Onion Service and user's computer are connected, there are six nodes between them: the guard node selected by the user's computer, one middle node, the rendezvous node, two middle nodes, and the guard node selected by the Onion Service. Only the Onion Service's guard node is aware of the Onion Service's IP address, and only the user's guard node is aware of the user's IP address.

Improvements in the Tor network's design and operation prior to May 2019 have made traffic analysis less reliable and more difficult to execute

12. Traffic analysis of Tor has always been unreliable because of security features which were present in Tor since its creation. For example, data sent between nodes has always been padded so that everyone's communications are the same size. As a result of this and other security measures, in 2012, NSA documents showed that "with manual analysis we can de-anonymize a very small fraction of Tor users."[2]
13. The Tor Project is continually improving the Tor network and associated software to enhance the level of privacy and usability offered to Tor users. This work is

---

[1] The IP address could allow the physical location of the Onion Service to be found.

[2] Tor Stinks, presentation by National Security Agency, dated June 2012. Published by The Guardian, October 4, 2013. Available at https://edwardsnowden.com/2013/10/04/tor-stinks-presentation/ (emphasis in original)

conducted in collaboration with academic researchers and other organizations. To help build trust in the development process, discussions of proposed and implemented changes to the Tor network are conducted publicly through academic literature, mailing lists, Internet chat, and websites maintained by the Tor Project. As such, the changes discussed here and the time frame in which they occurred are widely known.

14. Since September 2014, the Tor software will select one guard node and keep this selection for as long as possible to minimize the number of computers with knowledge of IP addresses. For this reason, if a Tor node collected IP addresses of users connecting to it, only a very small proportion of Tor users would be identified, no matter how long this node was run. It takes 68 days before a new node can run at full capacity, which is a measure put in place to prevent someone from quickly creating new nodes in an attempt to collect more IP addresses.
15. The likelihood that the Tor software will select any given node is proportional to that node's contribution to the capacity of the Tor network. Therefore, as the capacity of the Tor network has grown, the less likely it is that any one node will be selected, so it makes it less likely that a particular node can be used to observe users of the Tor network. For example, in 2012, NSA documents showed that "with manual analysis we can de-anonymize a very small fraction of Tor users."[3] Since then, the network capacity has grown from about 10 gigabits per second to 200 gigabits per second, which has further increased the difficulty of performing traffic analysis by a factor of 20.
16. Tor's encryption ensures that the content of data sent to and from a user's guard node is impossible to match to the corresponding content of data sent to or from the Onion Service's guard node. In other words, looking at the content of data the user sends to their guard node will be of no help in identifying with which Onion Service that user is communicating.

---

[3] Tor Stinks, presentation by National Security Agency, dated June 2012. Published by The Guardian, October 4, 2013. Available at https://edwardsnowden.com/2013/10/04/tor-stinks-presentation/ (emphasis in original)

17. Traffic analysis is a technique to attempt nevertheless to identify which user is communicating with which Onion Service by comparing patterns of when and how much data is sent (as opposed to looking at the content of the data, which is not visible to observers).
18. Prior to 2016, traffic analysis on Tor was unreliable, but there were concerns that it might be possible in some cases because the rate at which data was sent between the user and their guard node was similar to the rate at which data was sent between the Onion Service and its guard node. Prior to 2016, if someone were able to observe those two links simultaneously, patterns in the two rates of data transfer may be sufficiently similar to identify the link with some degree of confidence. That was no longer the case beginning sometime in 2016.
19. In 2016 Tor introduced an extension to its padding feature, to obscure patterns in the rate of data transfer to and from guard nodes. The Tor software randomly sends additional padding data to and from guard nodes which does not continue on through the rest of the Tor circuit. In so doing, the Tor software hides patterns in data rates that might otherwise allow traffic analysis to link users to the Onion Services they are visiting. Padding will cause traffic analysis to introduce more errors, both false-positives (where a user is incorrectly identified as having visited the Onion Service) and false-negatives (where a user is incorrectly identified as not having visited the Onion Service). In an undated presentation published in 2014,[4] GCHQ noted a high level of errors in performing traffic-analysis on Tor, even before the extended padding feature was introduced in 2016.
20. The nodes that make up the Tor network are operated by thousands of volunteers around the world, many of whom do not disclose their identities. In some cases, operators of Tor nodes were found to tamper with or observe traffic on the nodes. To prevent operators from being able to tamper with or observe traffic passing through

---

[4] A potential technique to deanonymise users of the TOR network (undated). Published by Der Spiegel, December 28, 2014. Available at https://edwardsnowden.com/2015/01/07/a-potential-technique-to-deanonymise-users-of-the-tor-network/

their node, since 2014, the Tor Project has pro-actively identified Tor nodes that show suspicious behavior and then exclude them from the network. This has increased the difficulty of covertly performing traffic analysis on the Tor network since 2014.

21. Thus, prior to May 2019, numerous measures were implemented in the Tor software to make it even more difficult to use traffic-analysis to de-anonymize Tor users.

Law-enforcement likely had control over the Onion Service when the visit was recorded

22. Law enforcement can attempt to identify the IP address of a Tor user visiting an Onion Service in four scenarios:
    1) Law enforcement controls neither the user's guard nor the Onion Service
    2) Law enforcement can observe the user and observe the Onion Service
    3) Law enforcement controls the Onion Service and some guard nodes
    4) Law enforcement controls the Onion Service
23. Although I describe four scenarios, there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a Network Investigative Technique (which interferes with a user's computer).

Scenario 1: Law enforcement controls neither the user's guard nor the Onion Service

24. In the first scenario, law-enforcement can only use traffic analysis if both the Onion Service and the user happen to randomly select a guard node controlled or observed by law-enforcement. Because guard nodes are selected at random, the chance of simultaneously controlling or observing both guard nodes is very small. It is for this reason, I believe the NSA concluded in 2012 that reliably de-anonymizing Tor users was not feasible, and since then, the difficulty has increased.

Scenario 2: Law enforcement can observe the user and observe the Onion Service

25. In the second scenario, law-enforcement could use traffic analysis to confirm if a particular user was visiting an Onion Service. For example, in the complaint dated October 29, 2014, alleging that Blake Benthall operated the Silk Road 2.0 Onion

Service,[5] the FBI noted similarities between Tor traffic observed through pen-register data at the defendant's residence and activity on the Onion Service in question. There are still likely to be errors in traffic-analysis because of Tor's padding obscuring patterns in the rates of data, leading to both false-positives and false-negatives.

Scenario 3: Law enforcement observes the Onion Service and some guard nodes

26. In the third scenario, law-enforcement can use traffic analysis to try to identify random visitors to an Onion Service (as opposed to specific targets). Traffic analysis is more likely to succeed than in the first scenario, but the likelihood of doing so is still very small. Firstly, it would only be possible to trace users who happen to select a guard under observation by law-enforcement. Secondly, even in the small number of cases where this has occurred, Tor's padding will cause traffic analysis performed through observing traffic to have a significant number of errors. Even if there are similarities in traffic patterns at a given guard node under observation and at the Onion Service, it could be that a different guard node is the correct match but is not under observation. As the number of visitors to an Onion Service increases, so will the likelihood of traffic analysis errors. Increasing the traffic to an Onion Service to frustrate traffic analysis is known as adding "cover traffic." To reduce the chances of errors, law-enforcement should wait until traffic-analysis indicates that the same user has visited an Onion Service multiple times.

Scenario 4: Law enforcement controls the Onion Service

27. In the fourth scenario, law-enforcement could use a Network Investigative Technique (NIT) to identify the IP address of a user visiting an Onion Service by forcing the user's computer to disclose its IP address by connecting directly to a law-enforcement server without using the Tor network.

---

[5] United States of America v. Blake Benthall, Southern District of New York. October 29, 2014. Available at https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/Benthall,%20Blake%20Complaint.pdf

28. In order to use an NIT, law-enforcement must control the Onion Service prior to deploying the NIT. If law-enforcement controls the Onion Service, applying an NIT would be feasible and avoid the error-prone nature of traffic analysis.
29. An NIT used in such a scenario could be based around malware that executes on the user's computer and forces it to directly connect to the Internet (as opposed to connecting through Tor). The FBI used this technique to identify visitors to the Freedom Hosting servers.[6] Such an NIT causes the user's computer to do something it would not otherwise do and therefore interferes with the user's computer.
30. Alternatively, the NIT may not involve malware code and instead force the user's Tor Browser to malfunction and connect directly through the Internet rather than sending network traffic through the Tor network. Such an NIT causes the Tor Browser on the user's computer to malfunction and reveal information that it was designed not to, and therefore interferes with the user's computer.
31. In summary, I do not believe the first scenario is plausible for this case. Traffic analysis is extremely unlikely to yield the hundreds of IP addresses submitted by the [redacted], nor give the [redacted] confidence that these IP addresses visited the Onion Service in question.
32. I, therefore, conclude that law-enforcement almost certainly controlled the Onion Service prior to May 23, 2019, and either used traffic analysis or an NIT to identify visitors to the Onion Service. As discussed above, a single identification using traffic analysis could very well be a false-positive error. An NIT necessarily interferes with a user's computer wherever it is located.

[6] Feds Are Suspects in New Malware That Attacks Tor Anonymity, Kevin Poulsen, Wired News, August 5, 2013. Available at https://www.wired.com/2013/08/freedom-hosting/

Neither of the two papers that Special Agent Ford cites could explain what has happened in this case

33. For reasons discussed below, neither of the two papers cited by Special Agent Ford, in paragraph 7 of the declaration dated August 10, 2020, could explain what has happened in this case.

The existence of research on how to defend against a global passive adversary does not imply a global passive adversary is a realistic threat

34. Neither paper shows that a global-passive adversary is possible.
35. Information security research commonly makes use of unrealistic and hypothetical scenarios to help ensure that systems are secure in all realistic scenarios. This approach is analogous to that taken for systems where a failure would be dangerous, such as elevators. These are designed to withstand a weight far exceeding what is realistic (or even possible) so as to create a safety margin when they are used in the real world.
36. The global-passive adversary is a similar type of theoretical assumption. A global-passive adversary is a hypothetical single organization that can observe every computer and every network connection in the world simultaneously and record all information. This is impossible, and even the most capable intelligence agencies such as NSA or GCHQ cannot achieve this goal.
37. The global-passive assumption is a helpful thought experiment for research because if a system is designed to be secure even in the face of a global-passive adversary, then it should be safe in any realistic situation. The use of the global-passive adversary assumption in research does not, however, imply that such an adversary could ever exist in the real world.

The method of traffic-analysis that Special Agent Ford cites was not a feasible method in this case

38. The 2008 paper cited by Special Agent Ford in paragraph 7 of his declaration, by Chakravarty et al., assumed that the IP address of the user visiting the Onion Service was already known to law-enforcement and that law-enforcement were able to

manipulate network equipment that is carrying that user's traffic only to confirm that identification. This confirmatory technique only worked when the law-enforcement agency was on the same continent as the user, and even then, it was unreliable. Since 2008, this type of confirmatory technique has become much more difficult for the reasons discussed above. The 2008 paper is not relevant to understanding what law-enforcement could have done in 2019.

The Tor Project's advice has been taken out of context

39. The Special Agent's citation in paragraph 5, to the Tor Project's advice to its users has been taken out of context. It continued:

> *"First, Tor protects the network communications. It separates where you are from where you are going on the Internet. What content and data you transmit over Tor is controlled by you. If you login to Google or Facebook via Tor, the local ISP or network provider doesn't know you are visiting Google or Facebook. Google and Facebook don't know where you are in the world. However, since you have logged into their sites, they know who you are. If you don't want to share information, you are in control.*
>
> *Second, active content, such as Java, Javascript, Adobe Flash, Adobe Shockwave, QuickTime, RealAudio, ActiveX controls, and VBScript, are binary applications. These binary applications run as your user account with your permissions in your operating system. This means these applications can access anything that your user account can access. Some of these technologies, such as Java and Adobe Flash for instance, run in what is known as a virtual machine. This virtual machine may have the ability to ignore your configured proxy settings, and therefore bypass Tor and share information directly to other sites on the Internet. The virtual machine may be able to store data, such as cookies, completely separate from your browser or operating system data stores. Therefore, these technologies must be disabled in your browser to use Tor safely.*
>
> *That's where Tor Browser comes in. We produce a web browser that is preconfigured to help you control the risks to your privacy and anonymity while browsing the Internet. Not only are the above technologies disabled to prevent identity leaks, Tor Browser also includes browser extensions like NoScript and*

Torbutton, as well as patches to the Firefox source code. The full design of Tor Browser can be read here. In designing a safe, secure solution for browsing the web with Tor, we've discovered that configuring other browsers to use Tor is unsafe."

40. First, Tor does not protect users from disclosing identifying information about themselves (e.g., name, email address), but in this case, there is no allegation that the Internet user ever logged into any website or revealed their email address in a way that allowed law-enforcement to identify them.
41. Second, the Tor Project advises users to use Tor Browser when connecting to Tor because the Tor Browser disables technologies that could disclose identifying information.
42. The advice from the Tor Project that Special Agent Ford cites does not discuss traffic analysis or the global passive adversary at all.
43. This guidance from the Tor Project does not mean that the theoretical scenarios Special Agent Ford outlined in his declaration are likely or even possible. In fact, when highly capable intelligence agencies have tried to de-anonymize Tor users, they have rarely succeeded.
44. The discussion by Special Agent Ford on tracing exit nodes, in paragraph 6, is also not relevant to the case. Exit nodes are only used when Tor users visit a website outside of the Tor network. When visiting a Tor Onion Service, an exit node is not used because data never leaves the Tor network.

Using a Tor search engine to visit an Onion Service website is easy

45. Paragraph 27 of the search warrant affidavit implies that searching to discover the address of an Onion Service is difficult and requires the use of a directory site.
46. In fact, entering "tor search" into the Tor Browser address bar (as of June 2021) will offer 5 different search engines for Tor Onion Services, allowing the user to find Onion Services matching particular keywords easily. Of these, at least two were available in May 2019. There is no need to use an index to find a Tor Onion Service because search engines are easily available from Tor Browser with just a few clicks.
47. Compared to the open Internet, there are fewer Onion Services, and so it is easier for a user to visit all sites returned for a search. For example, a search on the Torch search

engine for "Department of Justice" finds 61 Onion Service websites, so it would be easy to visit them all. In contrast, Google finds 107 million websites, and so there is no feasible way to visit all of these.

Visiting an Onion Service from a search engine does not imply the visitor was aware of the content of the website

48. Search engines, including for Onion Services, build an index of websites and associate these with keywords. This index is built by the search engine visiting publicly accessible parts of the website. Material on the website that is only visible after logging in will not be part of this index. Based on the screenshot of the target website's homepage, the site's homepage did not indicate the nature of the content available to logged-in users. Therefore the target site may appear in searches for innocuous keywords. Furthermore, when the site appears in search results, it will likely not be possible for a user to identify that there is illegal content without clicking on the search result to visit the website. For example, someone interested in BDSM could search for this term in a Tor search engine, but the results would not make clear what content is on the websites (see exhibit B attached, a search for "BDSM" as of June 2021 returning 10 results, any of which would be easy to click on).
49. Sites also have an incentive to encourage visitors from search engines, so the operator of the site may apply techniques to cause the site to appear more highly ranked for a wider range of keywords. This incentive results from the fact that some Onion Services are supported by advertising, just as with the open Internet. Furthermore, Onion Services who wish to protect the privacy of their operator and users visiting them may wish to increase the traffic to the website in order to obfuscate attempts to perform traffic analysis or other de-anonymization techniques (i.e., to add cover traffic). Search results may be intentionally misleading to attract more users who might not necessarily be interested in the content the website contains.

Directories will not necessarily indicate the content of a website

50. Paragraph 27 of the search warrant affidavit also implies that directories of Onion Service addresses give accurate and clear indications of whether these services contain unlawful material.

51. This is not necessarily the case. Some directories are open to editing by anyone and are not moderated. A person who wishes to promote an Onion Service may list the address while not indicating that the content is unlawful. As with the discussion of search engines above, this could be because, for example, the person wants to attract more users who are not motivated by illegal content but may nevertheless visit.

The difficulty of discovering the IP address of an Onion Service has nothing to do with how easy it is to visit an Onion Service

52. Paragraph 14 of the search warrant affidavit could be interpreted as saying that it is very difficult for users to view and visit Onion Services because they cannot find the IP address of the Onion Service using public lookups. However, this interpretation would not be correct.
53. Tor allows users to visit an Onion Service without knowing that service's IP address. Visiting an Onion Service from the Tor Browser is as simple as clicking on a link.
54. On the open Internet, law-enforcement can use a website's address (e.g., www.justice.gov) to identify its IP address. Tor does not allow law enforcement to do this for Onion Services. As a result, it is difficult, including for the reasons discussed above, for law enforcement to identify and locate who is running an Onion Service. That has nothing to do with how easy it is for a user to visit a Tor Onion Service because Tor allows users to visit an Onion Service without knowing its IP address.

A recorded visit to an Onion Service does not imply there was intent to visit that Onion Service or view the content on it

55. Just because someone visits a website, it does not imply that they intended to visit that website or view the content on that website.
56. It is common that a single website will contain parts of other websites. For example, on visiting the CNN homepage, content is downloaded from 70 different domain names, mostly for the purposes of showing advertisements or collecting statistics about who is visiting the site. The CNN homepage includes code that causes the web browser to download and display an image from Google to form part of an advertisement.

57. Onion Services can operate similarly. For example, an Onion Service (A) could include code that instructs Tor Browser to download images or other content from a different Onion Service (B), which then may or may not be displayed. If Onion Service B was under surveillance by law-enforcement, whether through an NIT or traffic analysis, a user visiting Onion Service A would also be seen to be visiting Onion Service B, even though the user only meant to visit Onion Service A. In the implementation of an NIT or traffic-analysis that I am aware of, it would not be possible for law-enforcement to distinguish someone directly visiting Onion Service B from someone who actually visits Onion Service A, which then triggers the indirect visit to Onion Service B.
58. Someone may include part of one Onion Service website within another to inflate the number of visitors to the website, to create cover traffic, to advertise content, or to collect statistics on who is visiting the site. The act of someone's browser visiting an Onion Service is not an indication of an intent to visit that website.

DONE this day, June 21, 2021.

Professor Steven Murdoch
Cambridge, UK

Exhibit A

Professor Steven J. Murdoch

Address: Computer Science Department
University College London
Gower Street, London, WC1E 6BT

Email: s.murdoch@ucl.ac.uk
Homepage: https://murdoch.is/

Education

2002–2007	University of Cambridge, Computer Laboratory (UK) – PhD in Computer Science Thesis: *Covert Channel Vulnerabilities in Anonymity Systems*
1998–2002	University of Glasgow (UK) – BSc Honours in Software Engineering (1st Class)

Professional History

Oct 20–	Professor (proleptic appointment), Computer Science, University College London
Oct 16–Oct 20	Reader (proleptic appointment), Computer Science, University College London
Aug 14–	Principal Research Fellow, Computer Science, University College London
Nov 13–	Innovation Security Architect, OneSpan
Dec 12–Jul 14	Research Fellow, Computer Laboratory, University of Cambridge
Jan 09–Nov 12	Senior Research Associate, Computer Laboratory, University of Cambridge
Aug 07–Sep 13	Chief Security Architect, Cronto
Aug 07–Dec 08	Research Associate, Computer Laboratory, University of Cambridge
Aug 06–Jun 07	Research Assistant, Computer Laboratory, University of Cambridge

Expert Witness

- Expert witness for Worcester Police Force, 2007
- R v Patel, Croydon Crown Court, 2008
- Job v Halifax PLC, case number 7BQ00307, Nottingham County Court, 2009
- Kaae v HSBC, London Mercantile Court, 2011
- R v Fisher, Camberwell Green Youth Court, 2014
- R v Vincent, Winchester Crown Court, 2014
- Expert witness relating to an application for third-party disclosure, 2014
- Ongoing case related to attribution of Internet traffic, 2019

Other Appointments and Affiliations

Fellowships:

- Fellow of the Institution of Engineering and Technology – FIET (2016–)
- Fellow of the British Computer Society – FBCS (2016–)
- Bye-Fellow, Christ's College Cambridge (2014–)
- Research Fellow, Christ's College Cambridge (2008–2014)

Journal Editor:

- Proceedings on Privacy Enhancing Technologies (2015)
- IEEE Internet Computing (special edition in 2013)
- SpringerBriefs in Cybersecurity (2012–)

International Award Chair:

- Andreas Pfitzmann (Privacy Enhancing Technologies Symposium) Award (2019)

International Conference Sponsorship Chair: Privacy Enhancing Technologies Symposium (2016–)

International Conference Program Chair: Privacy Enhancing Technologies Symposium (2014–2015)

International Conference General Chair: Financial Cryptography (2011)

International Conference Programme Committee Member:

- ACM CHI Conference on Human Factors in Computing Systems (2019)
- IEEE European Symposium on Security and Privacy (2019)
- Financial Cryptography (2010, 2016, 2018)
- IFIP Summer School (2008, 2016, 2017)
- Network and Distributed System Security Symposium (2017)
- ACM Conference on Computer and Communications Security (2007, 2008, 2010, 2011, 2016)
- Annual Privacy Forum (2014)
- USENIX Free and Open Communications on the Internet (2013)
- USENIX Security (2012)
- European Symposium on Research in Computer Security (2011)
- Privacy Enhancing Technologies Symposium (2007, 2008, 2009, 2011)
- Workshop on Foundations of Security and Privacy (2010)
- Workshop on Privacy in the Electronic Society (2006, 2007, 2009)
- ACM Symposium on Applied Computing (2007)

International Award Committee Member:

- SC Awards Europe (2018)
- PET Award (2013)

International Grant Proposal Reviewer:

- EPSRC Peer Review College
- Arts and Humanities Research Council
- Royal Society International Exchanges Panel
- Netherlands Organisation for Scientific Research (NWO)
- Austrian Science Fund (FWF)
- Isaac Newton Institute
- National Science Foundation
- Canada Foundation for Innovation
- Research Council of Norway (Panel Leader for Centre of Excellence Programme)
- European Commission
- United States Air Force Office of Scientific Research (AFOSR)

International Journal Reviewer:

- Proceedings on Privacy Enhancing Technologies (2017, 2018, 2019)
- ACM Transactions on Information & System Security
- IEEE Transactions on Software Engineering
- IEEE/ACM Transactions on Networking
- Identity in the Information Society

Prizes, Awards and Other Honours

2019 Awarded Internet Research Task Force Applied Networking Research Prize
2019 Shortlisted for UCL Provost's Public Engagement Awards
2016 Awarded SIIA CODiE prize for Best Identity & Access Security Solution for DIGIPASS for Apps

2015 Awarded Security Products New Product of the Year for DIGIPASS 760 authentication token
2014 Shortlisted for Cambridge Ring Company of the Year
2011 Shortlisted for the Lloyd's Science of Risk Prize – Chip and PIN is Broken
2010 Awarded the IEEE Award for Outstanding Paper in Security & Privacy – Chip and PIN is Broken
2008 Awarded the IEEE Award for Outstanding Paper in Security & Privacy – Thinking Inside the Box: System-Level Failures of Tamper Proofing
2008 Shortlisted for the Privacy Enhancing Technologies (PET) Award for Outstanding Research – Sampled Traffic Analysis by Internet-Exchange-Level Adversaries
2008 Awarded the European Research Consortium for Informatics and Mathematics (ERCIM) Security and Trust Management Working Group Prize for Best PhD Thesis – Covert Channel Vulnerabilities in Anonymity Systems
2007 Awarded the USENIX Security Prize for Best Student Paper – Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks
2006 Awarded the University of Cambridge Computer Laboratory Prize for the Most Notable Publication of 2006 – Low-Cost Traffic Analysis of Tor
2006 Shortlisted for the Privacy Enhancing Technologies (PET) Award for Outstanding Research – Low-Cost Traffic Analysis of Tor

Invited Talks

37 invited talks given since 2004, inc. 17 at international conferences and 12 keynotes

Jul 18 Royal Society – Privacy Enhancing Technologies
Feb 18 Royal Society UK-Netherlands Bilateral International Meeting – *Transparency enhancing technologies for accountable data science*
Dec 17 European Parliament – Sakharov Debate: is online privacy a human right?
Dec 17 ACI Worldwide – Age of Customer Consent, who owns the Customer Data
Nov 17 University of Edinburgh – Payment Security: Attacks & Defences
Aug 16 IFIP Summer School – Anonymity & Censorship-Free Communication
Nov 15 BT Insights, Adastral Park – *Anonymous Communications*
Sep 15 Information Security Forum – *Privacy by Design*
Dec 14 GCHQ Academic Centers of Excellence conference – *Cyber-security innovation*
Oct 14 [Keynote] Payment Knowledge Forum 2014, London, UK – *Payment Security: Attacks & Defences*
Jun 14 [Keynote] OWASP AppSec Europe 2014, Cambridge, UK – Anonymous Communications and Tor: History and Future Challenges
Nov 13 [Keynote] UK Cyber & Fraud Solutions, British Embassy, Switzerland – *Banking Security*
Sep 13 [Keynote] European Symposium on Research in Computer Security (ESORICS 2013), Royal Holloway, UK – *Security Protocols and the Law: The Case of Chip and PIN*
Sep 13 [Keynote] Quantitative Aspects in Security Assurance, (QASA 2013), Royal Holloway, UK – *Quantifying and Measuring Anonymity*
Mar 13 [Keynote] Open Web Application Security Project (OWASP), Leuven, Belgium – *Banking Security: Attacks and Defences*
Sep 12 [Keynote] Cryptographic Hardware and Embedded Systems (CHES 2012), K.U. Leuven, Belgium – *Banking Security: Attacks and Defences*
Jun 11 [Keynote] Centre for Telematics and Information Technology (CTIT) Symposium, University of Twente – *The Tor Anonymous Communication Network*
Feb 10 [Keynote] Conference on Achieving Sustainable Improvements in the Security of Retail Payments, Federal Reserve Bank of Philadelphia, Philadelphia PA, US – *Chip & PIN: 5 Years On*
Sep 08 [Keynote] Future of Identity in the Information Society (FIDIS)/International Federation for Information Processing (IFIP) Internet Security & Privacy Summer School, Brno, Czech Republic – *The Future of Anonymity and Censor-Free Publishing*
Jun 08 [Keynote] International Workshop on Security and Trust Management, European Research Consortium for Informatics and Mathematics (ERCIM), Trondheim, Norway – *On the Origins of a Thesis*
Sep 07 [Keynote] European Conference on the BSD Family of Operating Systems (EuroBSDCon), Copenhagen, Denmark – *Hot or Not: Fingerprinting Hosts through Clock Skew*

Teaching Career Summary

2015– Lecturer for University College London

- *COMP0057 Research in Information Security* (module co-ordinator, 30 contact hours over 10 lectures: lecturing and development of new lecture material)
- *COMP0064 Dissertation* (module co-ordinator, allocation of projects to supervisors and managing assessment; supervising and assessing MSc Information Security projects)
- *COMP0025 Introduction to Cryptography* (guest lecturer, on cryptography applied to banking security)
- *COMP0058 Applied Cryptography* (guest lecturer, on anonymous communications systems)

2014– Visiting Lecturer for Computer Science & Engineering at the University of Cambridge

- *Computer Security: Current Applications and Research* (lecturing, development of learning material, setting and marking of examinations for MPhil Advanced Computer Science)
- *Security II* (Lecturing, development of learning material, setting and marking of examinations for BA Computer Science course in Year 3 of 3)
- *Software Engineering* (Lecturer, Engineering Department for MEng Engineering in Year 3 of 4)

2002– Supervisor for Engineering and Computer Science at the University of Cambridge
Tutorials and marking of coursework for:

- *Digital Electronics* (BA/MEng Engineering course in Year 1 of 4)
- *Linear Circuits* (BA/MEng Engineering course in Year 1 of 4)
- Dimensional Analysis (BA/MEng Engineering course in Year 1 of 4)
- *Introduction to Security/Security I* (BA Computer Science course in Years 2 of 3)
- *Discrete Mathematics* (BA Computer Science course in Years 2 of 3)
- *Object Oriented Programming* (BA Computer Science course in Years 1 of 3)
- *Security II* (BA Computer Science course in Years 3 of 3)
- Computer Science undergraduate and diploma/MPhil (postgraduate) projects
- Engineering MEng projects

2014 Visiting Lecturer for Royal Holloway, University of London

- *Smart Cards/Tokens Security and Applications* (lecturing and development of new lecture and corresponding formative assessment, on Trusted Execution Environments)

2014 Visiting Lecturer for University College London

- *Web Economics* (lecturing and development of new lecture on Online Payments Methods)

2011–2014 Lecturer for Computer Science and Engineering at the University of Cambridge

- *Computer Security: Principles and Foundations* (Development of new course, lecturing, development of learning material, setting and marking of examinations for MPhil Advanced Computer Science)
- *Computer Security: Current Applications and Research* (Development of new course, lecturing, development of learning material, setting and marking of examinations for MPhil Advanced Computer Science)
- *Security II* (Lecturing, development of learning material, setting and marking of examinations for BA Computer Science course in Year 3 of 3)
- *Security I* (Lecturing, development of learning material, for BA Computer Science in Year 2 of 3)
- *Software Engineering* (Lecturer, Engineering Department for MEng Engineering in Year 3 of 4)

Enterprise/External Engagement

Creator and maintainer of the EMV Lab (https://emvlab.org/) research platform in 2009 providing tools for researchers and practitioners in the field of card and payment system security, **currently attracting over 32,000 visits per month.**

Creator of the Tor Browser in 2008 based on my research on Internet privacy. This system is now the flagship product of the Tor Project and the **technology used by the vast majority of Tor's 2 million daily users**.

Creator of the Cronto payment authentication technology, spun out from my banking research in 2007. I served as Chief Security Architect for this company until its acquisition by OneSpan in 2013. The technology is used **banks including market leaders in Germany, Netherlands and Switzerland**.

Short Courses for Professional Development:

- UCL Faculty of Laws – development of a new lecture covering topics including data protection, privacy enhancing technologies, blockchain, and cryptography for legal professionals (2016–)
- SecAppDev Industrial Training course jointly run by K.U. Leuven, Solvay Business School and Trinity College Dublin. Development of new series of lectures: *security economics; anonymity systems requirements and architecture; banking security architecture; ATM and point of sale system security architecture; online banking security* (2010–2014)
- University of Cambridge – development of lectures and practical exercises for an advanced course for information security practitioners in industry: *mobile systems; traffic analysis and anonymity* (2008–2010)

Information Security consultant:

- A hedge fund developing new internal security controls (2018)
- A fund investing in Internet security technologies (2017)
- A start-up developing and commercializing privacy enhancing technologies (2015–)
- A leading academic publisher (2015)
- A company developing secure collaboration tools and services (2013)
- A small company developing secure voice conferencing services (2010)
- Documotion Research, developing secure PIN distribution technologies (2005)
- A leading developer of mobile phone operating systems (2004)

Public and Policy Engagement:

- Member of Advisory Council to the Foundation for Information Policy Research (2019–)
- Contributor to UK Authorised Push Payment Contingent Reimbursement Model consumer protection scheme, including through advising Which? and Age UK on how my research shows how to prevent fraud (2016–2019)
- Author of Home Office standard for secure handling of evidence in the UK justice system (2014–2017)
- Steering group member for Royal Society report on Cybersecurity (2014–2016)
- Technical adviser to House of Commons Science and Technology Committee investigation on the Investigatory Powers Bill (2016)
- Organiser of joint Royal Society & Royal Society of Canada Frontiers of Science meeting on Information and Communication Technologies (2016)
- Editor of Parliamentary Office on Science and Technology report on The Dark Web (2015)
- Witness to the Joint House of Lords and Commons Committee on the Communications Data Bill (2013)
- Editor of Parliamentary Office on Science and Technology report on Digital Identity (2012)
- Frequent meetings with policymakers, working as a Member of the Cambridge Centre for Science and Policy (CSaP) Network (2010–)
- Author of first UK standard on secure distribution of payment card PINs (2005)

Outreach to schools and school-age students:

- Presenter at Royal Institution Engineering Masterclass at University of Cambridge and University of Oxford (2016–)

- Presenter at Royal Institution Computing Masterclass at UCL (2015–)
- Presenter at Royal Institution Maths Masterclass, Cambridge (2011–)
- Supervisor for Nuffield Research Placement (2013)
- Talks to the general public and school students, including during UK National Science & Engineering Week

Work with the media

- Research featured on Computerphile YouTube channel (57,665 views as of October 2019)
- Ran security and source-protection training for Channel 4 investigative journalists
- Author for The New Statesman; article in August 2017
- Author for The Daily Mail; article in August 2016
- Author for The Observer; article in April 2015
- Author for The Conversation; 7 articles with 121,000 readers since February 2015
- Author for The European; article in August 2011
- Reviewer for BBC Tomorrows World online activity on history of science
- Regular interviews with print, online, radio, and TV journalists, including:

The UK – New Scientist, The Times, Guardian, Telegraph, Independent, Financial Times, Daily Mail, BBC News, BBC Watchdog, BBC Newsnight, BBC Fake Britain, ITV Manhunt, Naked Scientists, Rip Off Britain, BBC World Service, The Register, LBC
US – CNN, Wall Street Journal, Huffington Post, Pittsburgh Business Times, ABC News, WIRED
Canada – CBC News
France – Sciences et Avenir
Germany – ARD Plusminus, The European, Der Spiegel, Heise
Italy – L'Espresso
The Netherlands – VPRO Goudzoekers
Columbia – NTN24
Australia – ABC Background Briefing
China – Central China TV
Other international outlets – Channel News Asia, Al Jazeera, International Business Times

Selected Publications

For the full list of publications, see https://murdoch.is/papers

- Do You See What I See? Differential Treatment of Anonymous Users. Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, Damon McCoy. 2016 Network and Distributed System Security Symposium, San Diego, CA, US, 21–24 February 2016.
- Optimising node selection probabilities in multi-hop M/D/1 queuing networks to reduce latency of Tor. Steven Herbert, Steven J. Murdoch, Elena Punskaya. IET Electronics Letters Volume 50, Issue 17, pages 1205–1207, 14 August 2014.
- Impact of Network Topology on Anonymity and Overhead in Low-Latency Anonymity Networks. Claudia Diaz, Steven J. Murdoch, Carmela Troncoso. 10th Privacy Enhancing Technologies Symposium (PETS 2010), Berlin, Germany, 21–23 July 2010.
- An Improved Clock-skew Measurement Technique for Revealing Hidden Services. Sebastian Zander, Steven J. Murdoch. 17th USENIX Security Symposium, San Jose, CA, USA, 28 July–01 August 2008.
- Metrics for Security and Performance in Low-Latency Anonymity Systems. Steven J. Murdoch, Robert N.M. Watson. 8th Privacy Enhancing Technologies Symposium (PETS 2008), Leuven, Belgium, 23–25 July 2008.
- Sampled Traffic Analysis by Internet-Exchange-Level Adversaries. Steven J. Murdoch, Piotr Zieliński. 7th Workshop on Privacy Enhancing Technologies, Ottawa, Canada, 20–22 June 2007.

Exhibit B

AHMIA bdsm Search

About Ahmia Statistics Add Service i2p search Contact Blacklist

Any Time

Did you mean *best*?

Omitted very similar entries. Displaying 10 matches in 0.26 seconds. Page 1 of 1 .

BDSM Bank

BDSM Bank
hiddeiulowqgdh34ngrehlkkov3ijvsivjgvbj6e27w4pbr7qogghdyd.onion — 6 months, 2 weeks ago —

BDSM Bank

BDSM Bank
hiddencrztrqz2h6bjito56pzdamwvhwssnhhghfvumfebuk5aejtlad.onion — 5 months, 4 weeks ago —

BDSM Bank

BDSM Bank
hiddewjoaam33ayyoyc4rhtjcusy7amoxlkidqshr4yfjx4avib6cmqd.onion — 6 months, 2 weeks ago —

Porn Videos - XONIONS

XONIONS Porn Videos
xonionshe7zqqhzowf6pjybykjt3j7a4ipszianf2rttnwsyiigli7qd.onion — 0 minutes ago —

Spanking – Jo van Buren

No description provided
sh33jayxnq7af3i6.onion — 2 weeks, 6 days ago —

Recent questions in Sex and relationships - Hidden Answers

"That's not a really weird sex act; that's a really weird sex act" - Crocodile Dundee.
ru.answerh4rfo4zgi4ao7lzoukjflpbur4ldabarachwwhabbu4vkpvxyd.onion — 3 weeks ago —

HIDDEN MARKETPLACE

HIDDEN MARKETPLACE
hidden24qtvlgaxp.onion — 5 months, 2 weeks ago —

The page of links...

A link page to zoophile, furry and anthropomorphic content.
tssa3yo5xfkcn4razcnmdhw5uxshx6zwzngwizpyf7phvea3gccrqbad.onion — 2 weeks, 6 days ago —

PZA Boy Stories

No description provided

7h6xs7vpc2qlmm4r2oxfpme3xmj2zvorgu2gwxe6uvq47fk3463qzdad.onion — 6 days, 1 hour ago —

PZA: Quick Search

No description provided

pzaboystoravp2rz.onion — 4 weeks ago —